TEACHGEN AI LTD

DPIA Support Pack

Customer resource for schools and trusts

Version	**1.0**
Effective date	**5 May 2026**
Document owner	**James Leeson, Data Protection Officer**
Data protection hub	teachgen.ai/data-protection
Contact	dataprotection@teachgen.ai

This public DPIA support pack is adapted from the ICO DPIA process and template structure. It is designed to help schools and trusts complete their own controller-side DPIA for TeachGen AI. It is not legal advice and does not replace the Customer's own assessment, DPO advice, residual-risk decision or ICO-consultation decision.

Important status note

This document is a customer resource to help schools, multi-academy trusts and other education organisations complete their own Data Protection Impact Assessment for TeachGen AI.

It is adapted from the ICO's DPIA process and template structure. It is not legal advice and it is not a substitute for the Controller's own assessment. The Customer remains responsible for deciding:

- completion and approval of its own DPIA before deployment;
- the lawful basis for its own processing;
- whether special category data or children's data will be processed;
- what consultation is appropriate;
- whether residual risk is acceptable; and
- whether prior consultation with the ICO is required.

This public version is written so it can be shared with Data Protection Officers, IT leads, safeguarding leads, procurement teams and governors. It avoids operational details that would undermine security.

Sources used

This support pack has been prepared using the following sources:

- ICO guidance: Data Protection Impact Assessments (DPIAs), including "What is a DPIA?", "When do we need to do a DPIA?", "How do we do a DPIA?", "Do we need to consult the ICO?", and "Examples of processing likely to result in high risk".
- ICO sample DPIA template, version 0.4, published March 2018.
- UK GDPR Article 35, as reflected in ICO guidance.
- TeachGen AI Standard Data Processing Addendum v2.0, effective 3 May 2026.
- TeachGen AI Standard Service Agreement v2.2, effective 3 May 2026.
- TeachGen AI Privacy Notice v2.1, updated 5 May 2026.
- TeachGen AI Sub-processors page, current as of 3 May 2026.

The ICO notes that its DPIA guidance is under review following the Data (Use and Access) Act 2025. Controllers should check current ICO guidance before final sign-off.

TEACHGEN AI · DPIA SUPPORT PACK

Step 1 - Identify The Need For A DPIA

Project summary

The project is the deployment of TeachGen AI, a cloud-hosted Software as a Service platform providing AI-powered educational tools for teachers and school staff.

TeachGen AI supports content creation, lesson planning, assessment support, feedback drafting, report writing, communication drafting, classroom-management support, leadership and administrative planning, educational personas, chat, image generation and presentation generation.

The service is generally used by staff at schools and trusts. It is not directed at, or designed for direct use by, children. However, teachers may include information about students, parents, guardians or other stakeholders in prompts or generated content. The service is therefore capable of processing personal data relating to children and, depending on customer use, sensitive or highly personal information.

DPIA screening position

The ICO requires a DPIA where processing is likely to result in a high risk to individuals' rights and freedoms. The ICO also considers it good practice to do a DPIA even where the threshold is not clearly met.

For a school or trust deployment of TeachGen AI, Controllers should complete and approve a DPIA before deployment. For many deployments this is likely to be required, because the deployment involves:

Screening factor	Applicability to TeachGen AI deployment	DPIA implication
Innovative technology, including AI	TeachGen AI uses generative AI for text, images, resources and chat-style interactions.	ICO guidance identifies AI and machine learning as innovative technology. In an education deployment this should be treated as a DPIA trigger unless the Controller records a clear reason why the processing is not likely to be high risk.
Vulnerable data subjects	The platform may process personal data about children when teachers include student information in prompts, reports or resources.	Children's data is a high-risk indicator in ICO and WP29/EDPB guidance.
Sensitive or highly personal data	The platform is not designed for routine special category data, but users could enter information about learning needs, health, safeguarding, behaviour, family context or pastoral matters.	Schools should assess whether special category data or highly personal data is likely in practice.
Tracking or monitoring	TeachGen AI records login, usage and audit-log data for service delivery, security, support and analytics.	Usage logging is not pupil profiling, but it should be considered in the DPIA.
Automated decision-making with legal or similarly significant effects	TeachGen AI does not make automated decisions about students, staff or access to services. Users remain responsible for reviewing outputs.	This factor is not expected to apply if the Customer prohibits use of outputs as sole evidence for significant decisions.
Data matching or combining datasets	TeachGen AI does not combine Customer data with external datasets for profiling. Customer SSO identity data and platform usage data are used for access, security and service operation.	Not expected to be a high-risk factor, unless the Customer adds integrations or exports data into other systems.

Controller completion points

The Customer should record:

- the school or trust name;
- project owner;

- DPO or data protection lead;
- intended user groups;
- whether students will use the platform directly;
- whether staff will be permitted to enter identifiable student data;
- whether special category data may be entered;
- whether the deployment forms part of a wider AI strategy or education technology procurement; and
- the date at which the DPIA can still influence the deployment.

TEACHGEN AI · DPIA SUPPORT PACK

Step 2 - Describe The Processing

Nature of processing

TeachGen AI processes personal data to provide an AI-powered educational platform. Processing may include:

- collection and storage of authorised user account details;
- authentication through Microsoft Entra ID or Google Workspace SSO, where configured;
- routing user prompts and content to enterprise AI infrastructure providers for inference;
- generating AI outputs such as lesson plans, feedback, reports, presentations, images and written communications;
- storing user-created content and generated outputs during the service term;
- recording platform usage, audit logs and security events;
- providing customer support;
- billing and subscription administration; and
- maintaining backups, monitoring and security controls.

TeachGen AI states that Customer prompts, Customer content and generated outputs are not used to train, fine-tune, evaluate or otherwise improve AI models unless the Customer gives prior, specific and revocable written consent.

Scope of processing

The Customer determines what personal data is entered into the platform. TeachGen AI does not require personal data for tool functionality except for authentication, account administration, support, security and service delivery.

Expected categories of data include:

Data subject group	Data likely to be processed
Authorised users	Name, work email, role, department or subject area, school or institution, account settings, usage logs, content created in the platform, support communications.
Students	Indirect references included by authorised users in prompts, resources, feedback, reports, planning, support plans or communication drafts.
Parents, guardians and other stakeholders	Indirect references included by authorised users in communication drafts, reports, planning or administrative content.
Customer administrators	Account administration details, security logs, support records and billing contacts.

The service is not designed for the routine processing of special category data. If staff enter special category data, the Customer must identify an Article 9 condition and any required Data Protection Act 2018 Schedule 1 condition.

Context of processing

The deployment context is education. Schools and trusts are likely to process personal data about children and staff in a regulated setting. Children are a vulnerable data subject group, and educational records can affect opportunities, wellbeing and relationships with families.

The key contextual controls are:

- the service is sold to schools and used by staff;
- the service is not directed at children;
- teachers retain professional responsibility for reviewing and using outputs;
- the Customer controls access, acceptable use, staff training and local policy;
- TeachGen AI processes Customer data as Processor under its Standard DPA for school deployments; and
- sub-processors are listed at teachgen.ai/sub-processors.

Purpose of processing

The purposes of processing are:

- enabling secure access to AI-powered educational tools;
- generating educational materials, plans, assessments, reports, feedback and communications from user inputs;
- supporting teachers and school staff to save time and improve consistency;
- maintaining platform security and preventing unauthorised access;
- providing customer support and service communications;
- managing billing and contractual obligations;
- improving service quality through aggregated usage analysis; and
- complying with legal and regulatory requirements.

Data flow summary

1. An authorised user accesses TeachGen AI through the web platform.
2. The user authenticates, typically through school SSO where configured.
3. The user submits a prompt, instruction, file content or other input.
4. TeachGen AI routes the request to the relevant enterprise AI provider or internal service to generate the requested output.
5. The generated output is returned to the user for review and editing.
6. The user’s content and outputs may be stored in the platform during the contract term.
7. Usage logs, audit logs and support records are retained according to the DPA retention schedule.
8. On termination, content is available for export for 30 days and is deleted within 60 days, subject to statutory retention for billing and tax records.

Sub-processors and regions

The current sub-processors are published at teachgen.ai/sub-processors. At the time this support pack was prepared, the list included Microsoft Azure, Microsoft 365, Amazon AWS, Google Cloud Platform, Cloudflare, Twilio SendGrid, Resend, Stripe and Google Analytics.

TeachGen AI states that:

- AI inference takes place inside enterprise tenancies in EU regions;
- Customer data is not sent to OpenAI's direct API;
- international transfers for operational sub-processors use safeguards such as adequacy decisions, the UK IDTA, the UK Addendum to the EU SCCs, EU SCCs, and the EU-US Data Privacy Framework where the recipient is certified; and
- customers receive at least 30 days' notice before the addition or replacement of a sub-processor.

Retention summary

Data category	Active retention	Post-termination
Authentication and account records	Term of the agreement	Deleted within 60 days of termination.
User content, prompts and outputs	Term of the agreement	Available for export for 30 days; deleted within 60 days.
Platform usage and audit logs	12 months from event	Deleted within 60 days of termination.
Backup copies	Maximum 35 days rolling	Overwritten in normal backup cycle following termination.
Billing and tax records	Term of the agreement	Retained for 6 years under restricted access.

Security measures summary

TeachGen AI's DPA describes the following technical and organisational measures:

- encryption in transit using TLS 1.2 or above;
- encryption at rest using AES-256;
- restricted access on a need-to-know basis;
- SSO through Microsoft Entra ID or Google Workspace where configured;
- security monitoring and updates;
- backup and disaster recovery procedures;
- data-protection guidance on joining and refresher materials maintained by the DPO;
- confidentiality obligations for staff and contractors;
- written agreements with sub-processors;
- 30-day notice for sub-processor changes; and
- Security Incident notification to Customers without undue delay and in any event no later than 72 hours of becoming aware, to ensure Controllers can meet the 72-hour Article 33 notification deadline.

TEACHGEN AI · DPIA SUPPORT PACK

Step 3 - Consultation Process

Supplier consultation evidence

TeachGen AI has published or made available:

- Privacy Notice;
- Standard Data Processing Addendum;
- Standard Service Agreement;
- sub-processor list and change log;
- technical and organisational measures;
- AI training restrictions;
- retention schedule;
- support and breach notification commitments; and
- this DPIA support pack.

Customers can contact dataprotection@teachgen.ai for additional due diligence, signed copies or security questionnaires.

Customer consultation to complete

The Customer should decide whether to consult:

- Data Protection Officer or data protection lead;
- IT or information security lead;
- safeguarding lead;
- senior leader responsible for teaching and learning;
- curriculum or assessment leads;
- staff representatives or pilot users;
- parents, students or governors where proportionate;
- procurement or legal advisers; and
- any local authority, trust central team or sector body with relevant policy oversight.

The Customer should document the views received and how those views changed the deployment plan.

DPO advice record

The Customer should record:

Question	Customer response
Was DPO advice sought?	To be completed by Customer.
Date advice was sought	To be completed by Customer.
Summary of DPO advice	To be completed by Customer.
Has the deployment been changed in response?	To be completed by Customer.
If DPO advice was not followed, why not?	To be completed by Customer.

TEACHGEN AI · DPIA SUPPORT PACK

Step 4 - Assess Necessity And Proportionality

Purpose and alternatives

The Customer should assess whether TeachGen AI is necessary and proportionate for its intended purposes. Relevant considerations include:

- whether the service supports a legitimate educational or operational need;
- whether comparable outcomes could be achieved without processing personal data;
- whether staff can use the service effectively with anonymised or pseudonymised examples;
- whether local policy restricts use of identifiable student data;
- whether existing school systems already provide similar functionality;
- whether the service reduces workload without reducing professional judgement; and
- whether any direct use by children is excluded or separately assessed.

Lawful basis

TeachGen AI cannot determine the Customer's lawful basis for school-controlled processing. The Customer should record the lawful basis for each category of use.

Common candidates for schools may include:

- Article 6(1)(e), public task, for state schools performing education functions;
- Article 6(1)(f), legitimate interests, for independent schools or non-public-task processing where applicable;
- Article 6(1)(b), contract, for account administration with individual subscribers; or
- Article 6(1)(c), legal obligation, for records required by law.

Where special category data is entered, the Customer must identify an Article 9 condition and any required Data Protection Act 2018 Schedule 1 condition.

Data minimisation

Recommended Customer controls:

- tell staff not to enter identifiable student data unless necessary;
- use initials, class groups or pseudonyms where possible;
- prohibit unnecessary inclusion of health, safeguarding, behaviour, SEND or family-context information;
- use school-approved templates for high-risk tasks;
- avoid uploading source documents containing more personal data than needed;
- restrict access to authorised staff only; and
- periodically review saved content and delete what is no longer needed.

Transparency

The Customer should ensure privacy information explains:

- that approved staff may use TeachGen AI to generate or support educational materials and communications;
- what categories of personal data may be used;
- that TeachGen AI acts as Processor for school-controlled platform data;

- that AI outputs are reviewed by staff before use;
- that Customer data is not used for AI model training;
- how individuals can exercise data protection rights; and
- where further information can be found.

Rights and human oversight

The Customer should maintain procedures for access, rectification, erasure, restriction, portability, objection and complaints. TeachGen AI's DPA says it will assist the Customer with data subject requests.

The Customer should prohibit use of TeachGen AI as the sole basis for decisions that have legal or similarly significant effects on individuals. Human review should be required before any output is used in:

- assessment or feedback with significant consequences;
- reports sent to parents or guardians;
- behaviour, safeguarding, pastoral or SEND documentation;
- performance management;
- admissions, exclusions or disciplinary processes; or
- formal records.

Processor management

The Customer should review and retain:

- Standard DPA v2.0;
- sub-processor list and change log;
- technical and organisational measures;
- breach notification commitments;
- audit and questionnaire commitments;
- deletion and export commitments; and
- transfer safeguards for any non-UK/EEA sub-processors.

TEACHGEN AI · DPIA SUPPORT PACK

Step 5 - Identify And Assess Risks

Risk ratings below are a starting point for Customer review. The Customer should adjust likelihood and severity based on its own deployment model, user groups, policy controls and training.

Risk register

Staff enter excessive identifiable student data into prompts or documents

- Source: user behaviour; unclear local policy.
- Potential impact: loss of control over personal data; unnecessary exposure of children's data.
- Inherent risk: high.
- Existing / recommended measures: staff acceptable-use policy; training; data-minimisation guidance; use pseudonyms or initials; avoid identifiable data unless necessary; retention controls.
- Residual risk: medium.

Staff enter special category or safeguarding data without a proper lawful basis or safeguards

- Source: pastoral, SEND, health, safeguarding or behaviour use cases.
- Potential impact: confidentiality breach; distress; unfair use of sensitive information; regulatory non-compliance.
- Inherent risk: high.
- Existing / recommended measures: Customer Article 9 and Schedule 1 assessment; restrict high-risk use cases; require senior or DPO approval for sensitive use; apply enhanced access controls.
- Residual risk: medium.

AI output is inaccurate, biased, inappropriate or misleading

- Source: generative AI limitations; prompt ambiguity; model behaviour.
- Potential impact: unfair treatment; reputational damage; poor educational decisions; distress.
- Inherent risk: high.
- Existing / recommended measures: human review before use; output warnings; staff training; do not rely solely on AI for significant decisions; report systematic errors.
- Residual risk: medium.

AI output is used as the sole basis for a significant decision

- Source: misuse by staff; pressure to automate workload.
- Potential impact: legal or similarly significant effects; unfair assessment; inability to challenge decisions.
- Inherent risk: high.
- Existing / recommended measures: local policy prohibiting solely automated significant decisions; mandatory professional judgement; audit of high-risk workflows.
- Residual risk: low to medium.

Personal data is used to train or improve AI models

- Source: provider default terms; configuration error; unsuitable sub-processor terms.
- Potential impact: loss of control; unexpected reuse; confidentiality concerns.
- Inherent risk: high.

- Existing / recommended measures: TeachGen AI DPA Clause 1.13 prohibits training, fine-tuning, evaluation or model improvement using Customer data unless prior specific consent is given; enterprise API arrangements; sub-processor contractual controls.
- Residual risk: low.

Unauthorised access to Customer content or accounts

- Source: compromised accounts; misconfigured permissions; insider access; cyber attack.
- Potential impact: confidentiality breach; exposure of children's data or staff data.
- Inherent risk: high.
- Existing / recommended measures: SSO where configured; role-based access; need-to-know access; encryption in transit and at rest; monitoring; breach notification; Customer leaver process.
- Residual risk: medium.

International transfer safeguards are not understood or kept current

- Source: USA-located operational sub-processors; changes in certification or transfer law.
- Potential impact: reduced protection for personal data; compliance challenge; regulatory concern.
- Inherent risk: medium.
- Existing / recommended measures: DPA transfer clause; SCCs, UK IDTA, UK Addendum, adequacy or DPF where applicable; sub-processor change notice; Customer review of transfer mechanisms.
- Residual risk: low to medium.

Sub-processor change creates new risk

- Source: supplier addition or replacement of sub-processors.
- Potential impact: unexpected processing location or purpose; reduced assurance.
- Inherent risk: medium.
- Existing / recommended measures: published sub-processor page; 30 days' notice; Customer objection process; DPA flow-down obligations.
- Residual risk: low to medium.

Usage analytics or logs are perceived as staff monitoring

- Source: platform logs, feature usage and audit records.
- Potential impact: reduced trust; employment-relations concern; chilling effect.
- Inherent risk: medium.
- Existing / recommended measures: transparency to staff; limit use of logs to security, support and service improvement; restrict access to logs; define local policy on monitoring.
- Residual risk: low to medium.

Children use the platform directly without a separate assessment

- Source: local rollout decision or account sharing.
- Potential impact: age-inappropriate interaction; lack of child-specific transparency; increased Children's Code risk.
- Inherent risk: high.
- Existing / recommended measures: TeachGen AI states service is not directed at children; Customer should prohibit direct pupil use unless separately assessed and contractually approved; review Children's Code implications.
- Residual risk: low if prohibited.

Retention exceeds what is necessary for local purposes

- Source: saved content, prompts, outputs, logs and backups.
- Potential impact: unnecessary retention of children's or staff data.
- Inherent risk: medium.

- Existing / recommended measures: DPA retention schedule; export and deletion windows; Customer content review; deletion of unnecessary outputs; local retention policy.
- Residual risk: low to medium.

Data subject requests cannot be answered fully or promptly

- Source: distributed content across prompts, outputs, logs and school records.
- Potential impact: inability to exercise rights; delay; complaint risk.
- Inherent risk: medium.
- Existing / recommended measures: DPA assistance clause; Customer request workflow; identify system administrators; export capability; record where TeachGen AI content is reused in school systems.
- Residual risk: low to medium.

TEACHGEN AI · DPIA SUPPORT PACK

Step 6 - Identify Measures To Reduce Risk

The following implementation controls are recommended for school and trust deployments:

- Approve a staff AI acceptable-use policy before rollout. Owner: Customer. Status: to be completed.
- Tell staff not to enter identifiable student data unless necessary. Owner: Customer. Status: to be completed.
- Prohibit direct pupil use unless a separate assessment is completed. Owner: Customer. Status: to be completed.
- Require human review of all AI outputs before use. Owner: Customer. Status: to be completed.
- Prohibit use as the sole basis for significant educational, safeguarding, employment or disciplinary decisions. Owner: Customer. Status: to be completed.
- Define whether SEND, safeguarding, health or behaviour data may be entered and under what approval controls. Owner: Customer. Status: to be completed.
- Complete Article 9 and Schedule 1 assessment if special category data is expected. Owner: Customer. Status: to be completed.
- Configure SSO and align access with joiner, mover and leaver processes. Owner: Customer / TeachGen AI. Status: to be completed.
- Review sub-processor list and transfer safeguards. Owner: Customer. Status: to be completed.
- Add TeachGen AI to privacy notices or staff/student/parent transparency materials. Owner: Customer. Status: to be completed.
- Train staff on prompt minimisation, output review and escalation routes. Owner: Customer. Status: to be completed.
- Confirm data export and deletion process for termination. Owner: Customer / TeachGen AI. Status: to be completed.
- Record DPO advice and sign-off decision. Owner: Customer. Status: to be completed.

TEACHGEN AI · DPIA SUPPORT PACK

Step 7 - Sign Off And Outcomes

Supplier view

Based on the public TeachGen AI legal and data-protection materials reviewed for this support pack, TeachGen AI has documented controls for:

- processor obligations under Article 28;
- no AI model training on Customer data;
- sub-processor disclosure and notice;
- data retention and deletion;
- security measures;
- breach notification support;
- data subject rights assistance;
- AI output limitations and human review; and
- customer support for DPIAs and consultations.

No unmitigated high residual risk is identified from the supplier-side materials alone, provided the Customer implements appropriate local controls and prohibits high-risk misuse. The Customer must still complete its own assessment because risk depends heavily on local deployment, user training, categories of data entered and whether children or special category data are involved.

Customer residual-risk decision

The Customer should complete:

Decision	Customer response
Overall residual risk rating	To be completed by Customer.
Are any residual risks high?	To be completed by Customer.
If high risks remain, can they be reduced further?	To be completed by Customer.
Is prior consultation with the ICO required?	To be completed by Customer.
Date approved	To be completed by Customer.
Approved by	To be completed by Customer.
Review date	To be completed by Customer.

If the DPIA identifies a high residual risk that cannot be reduced, the Customer must consult the ICO before the processing goes ahead.

Review triggers

The Customer should review this DPIA if:

- TeachGen AI changes sub-processors or processing locations;
- new AI features materially change processing;
- pupils are given direct access;
- the Customer permits routine special category data processing;

- the Customer integrates TeachGen AI with other school systems;
- there is a significant security incident;
- ICO guidance changes materially; or
- local policy, law or public concern changes the risk context.

Document control

- **Version**: 1.0
- **Effective date**: 5 May 2026
- **Document owner**: James Leeson, Data Protection Officer, TeachGen AI Ltd
- **Review cycle**: Annual, or sooner if required by changes in law, ICO guidance, sub-processor arrangements, AI functionality or customer deployment model
- **Related documents**:
  - Privacy Notice: https://www.teachgen.ai/privacy-policy
  - Data Protection overview: https://www.teachgen.ai/data-protection
  - Standard Data Processing Addendum: https://www.teachgen.ai/standard-dpa-v2.0.pdf
  - Standard Service Agreement: https://www.teachgen.ai/standard-service-agreement-v2.2.pdf
  - Sub-processors: https://www.teachgen.ai/sub-processors
- **Contact**: dataprotection@teachgen.ai